

(12) UK Patent Application (19) GB (11) 2 358 948 (13) A

(43) Date of A Publication 08.08.2001

(21) Application No 0102621.0

(22) Date of Filing 02.02.2001

(30) Priority Data

(31) 9499507

(32) 07.02.2000

(33) US

(51) INT CL⁷

B42D 15/10 , G07F 7/10

(52) UK CL (Edition S)

G4H HTG H1A H13D H14A H14B H14D

B6A AC91 AK

G4A AAP

(71) Applicant(s)

Aztak Technology Corporation

(Incorporated in USA - Florida)

4208 West Sylvan Ramble Street, Tampa,
Florida 33609, United States of America

(56) Documents Cited

GB 2274184 A DE 029808147 U DE 019938001 A1
JP 030035384 A NL 001011708 C NL 001010221 C

(72) Inventor(s)

Allen John Keetch

Kenneth Edward Hines

(58) Field of Search

UK CL (Edition S) G4H HTG

INT CL⁷ B42D , G06F , G06K , G07F

Online: WPI, EPDOC, PAJ

(74) Agent and/or Address for Service

Nigel Brooks

Hill Hampton, East Meon, PETERSFIELD, Hampshire,
GU32 1QN, United Kingdom

(54) Abstract Title

Password storage apparatus and method

(57) A memory device 30 allows a person to remember only a single code and use that code to retrieve the identifying code or password required to access a secure facility. The memory device 30 is nearly the size and shape of a credit card and has a display 32, keypad 34, and housing 44, which may be tamper-proof, having a writing portion 46 on the rear. A user initially uses the keypad 34 to enter both a memory access code and a separate identifying code associated with each secure site or equipment. Subsequently, when the user desires to access a selected site or equipment (s)he can enter the access code and read, from the display, the required identifying code. A mnemonic descriptor can be written on a designated blank writing portion 46 on the housing, for each stored code. A brief advertising message can also be stored in the device memory and displayed each time the device is turned on. In a preferred embodiment, all the stored identifying codes are erased after a predetermined number of sequential inputs of the incorrect access code.

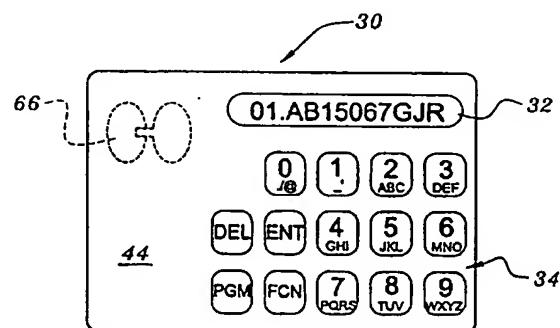


FIG. 1

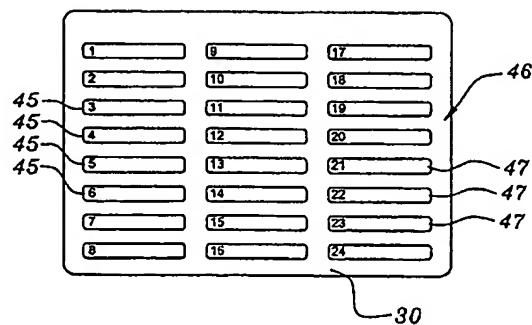


FIG. 2

GB 2 358 948 A

1/3

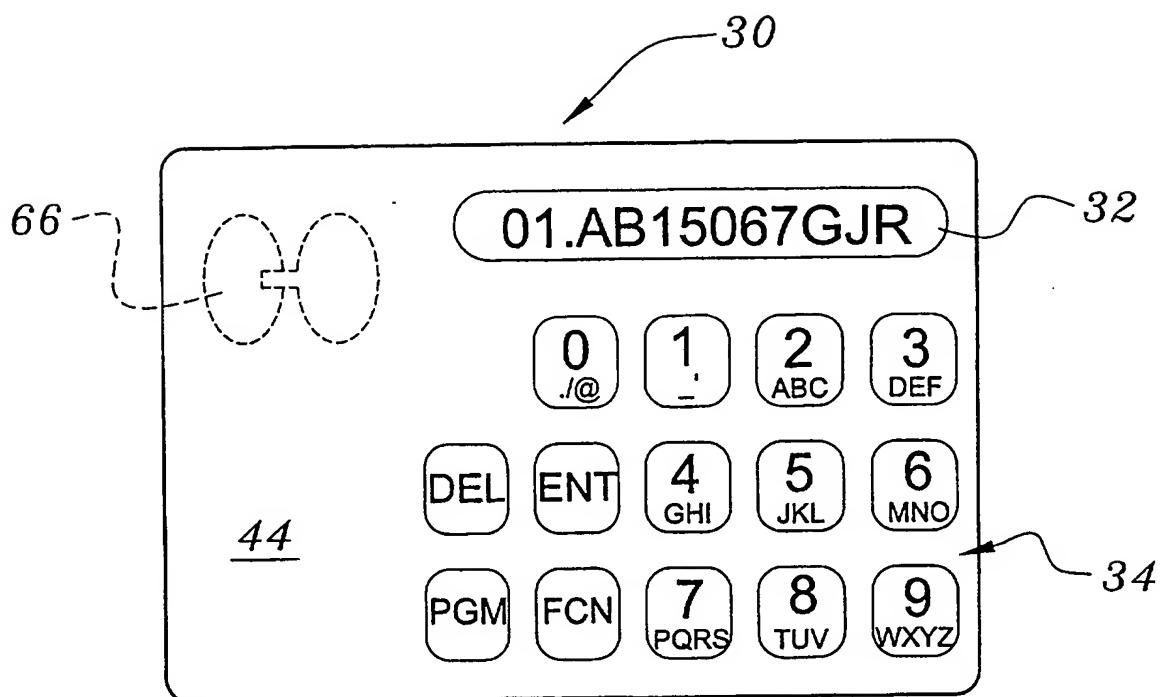


FIG. 1

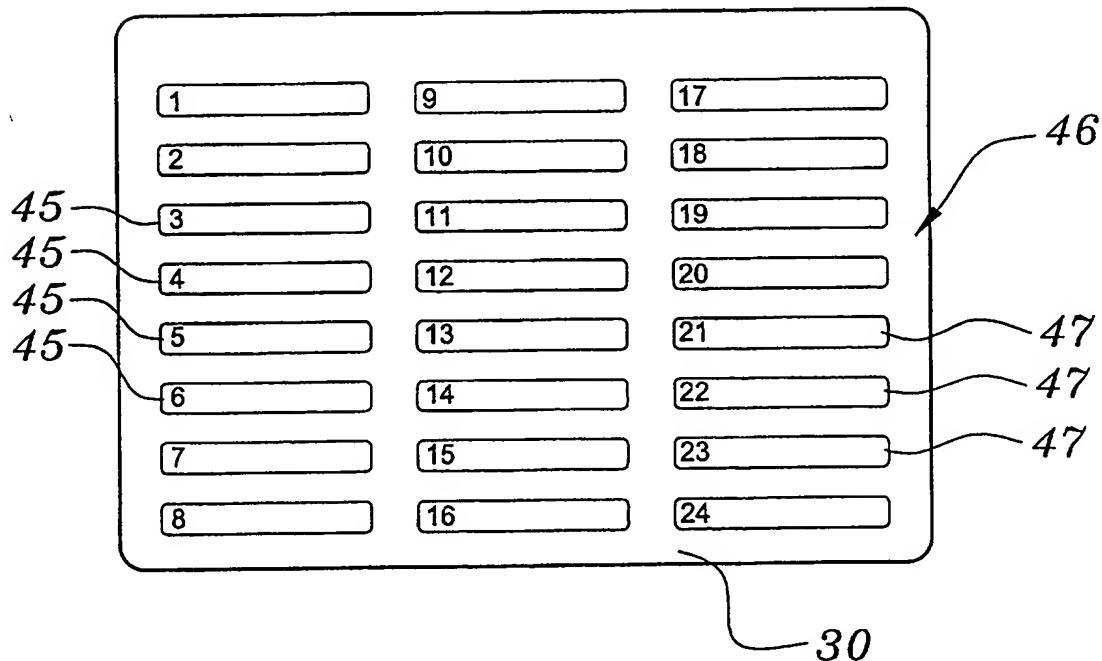


FIG. 2

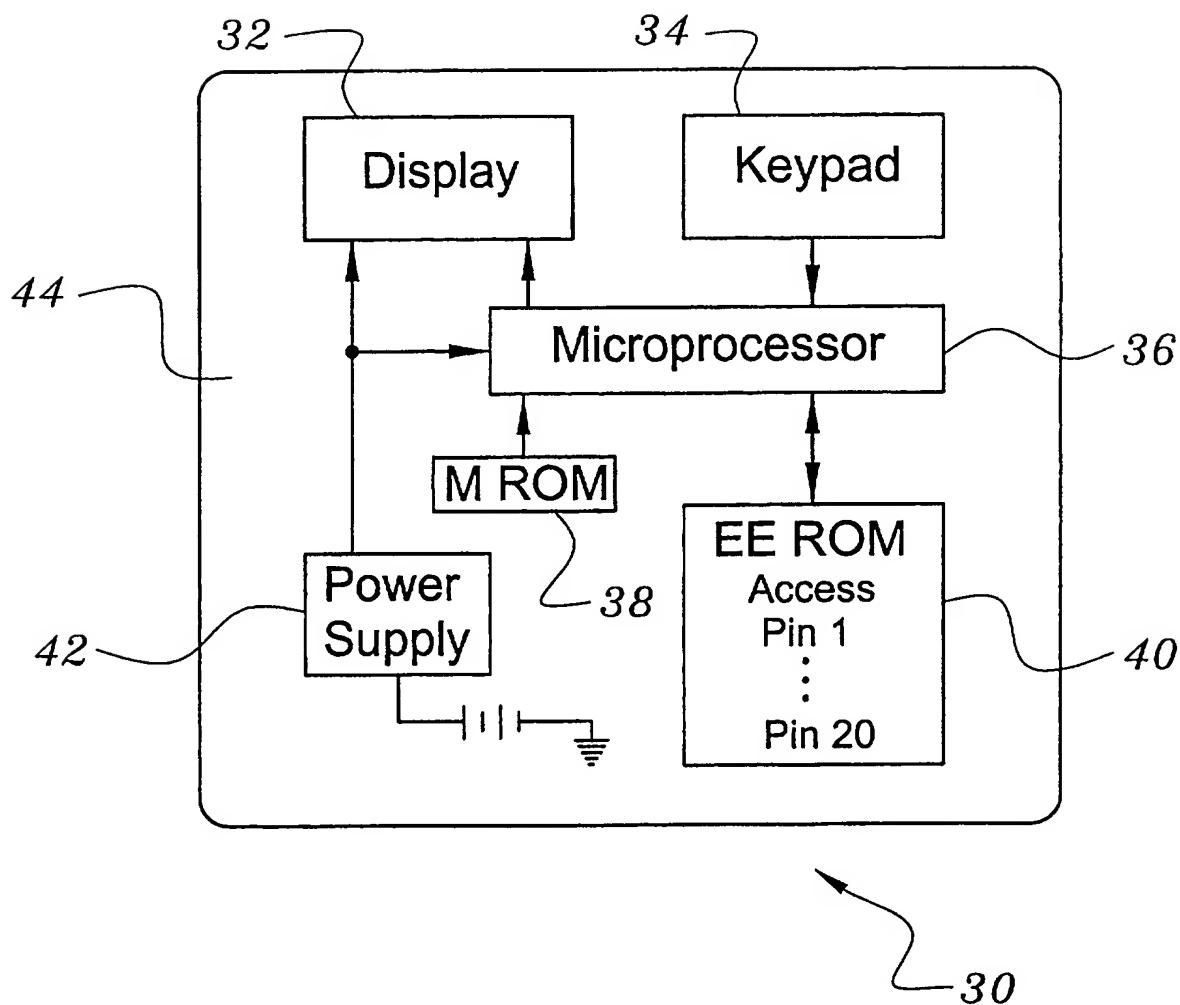


FIG. 3

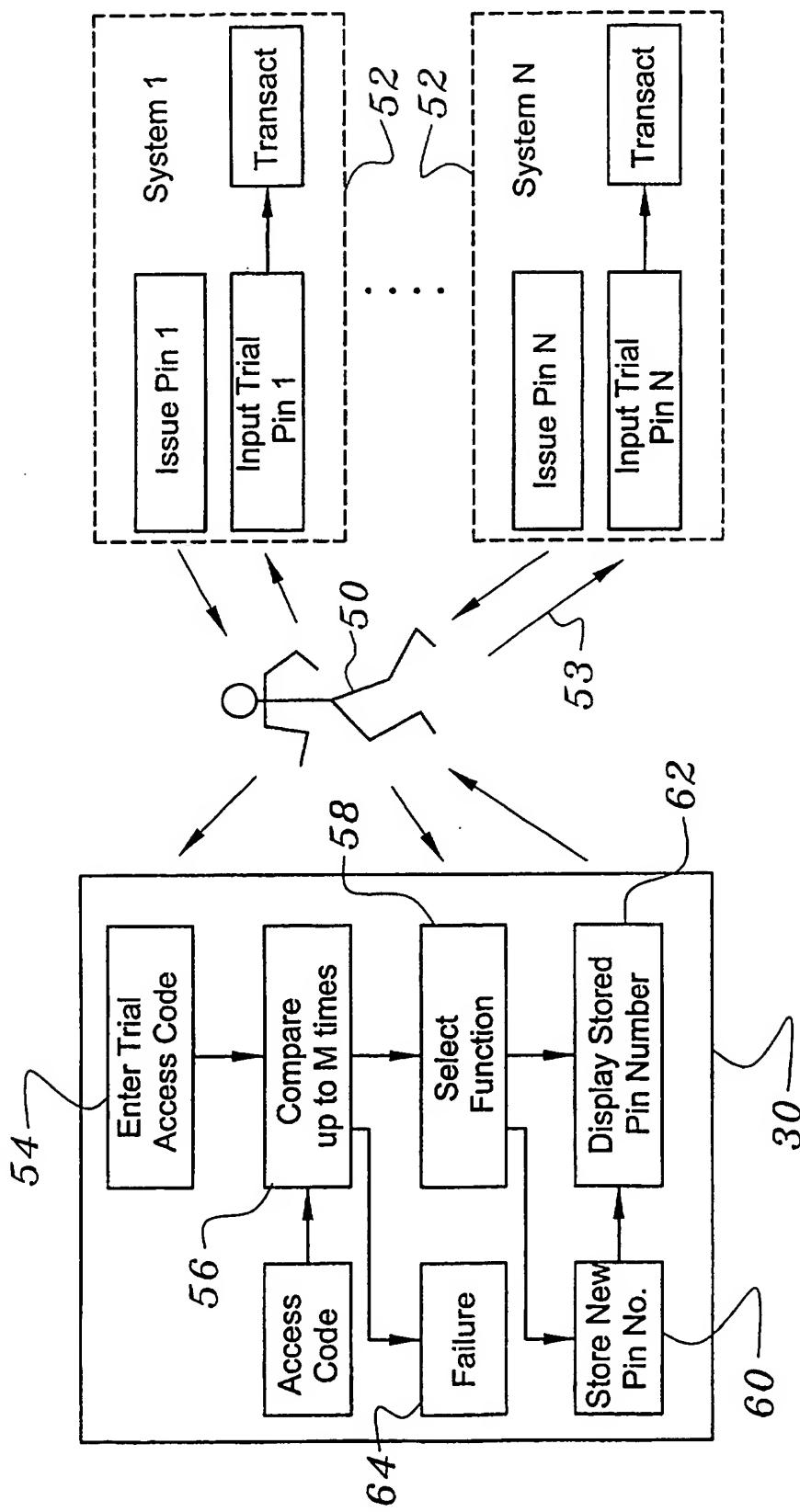


FIG. 4

PASSWORD STORAGE APPARATUS AND METHOD

The invention relates to security arrangements in which access to a transactional capability or to some physically secured location or object is granted
5 responsive to an authorised user providing a password, personal identification number or other unique message to identify himself. More specifically, the invention relates to secure means of storing passwords for use with multiple systems.

There are many arrangements in which a person must provide a password,
10 personal identification number (PIN), or some other user-identifying code to a secure apparatus in order to carry out a transaction or to be permitted physical access to a protected area or object. These arrangements include many credit and debit transactions (e.g., those carried out at automated teller machines), entry to an area locked by a combination lock or electronic access control means; and password access
15 to the use of a computer. In many such arrangements the secure system issues a Personal Identification Number (PIN) or other password to users. It is therefore common for many people in our society to have to remember and use multiple passwords, PINs and the like in order to get through an average day. A common problem in modern life is that of forgetting a password needed to carry out some
20 essential or important activity.

The level of security offered by the use of a password is often compromised by users who simply can not remember all their passwords and who write them down somewhere handy. Whenever one of these people has a purse or wallet stolen, there
25 is a high likelihood that the thief will discover the nominally hidden password and will try using that password with various credit cards, ATM cards, etc. in an attempt to steal more from the victim.

Several inventors have addressed the problems of password proliferation by
30 attempting to provide a secure means of password storage that a user can carry along with whatever physical record (e.g., a teller machine card) is needed for access. The patent art in this field includes:

* US 5,742,035, to Kohut, who teaches printing a matrix of numbers on the surface of a wallet card (e.g., a credit card, ATM card or the like). The PIN

associated with the card is made up of a sequential pattern of some of the numbers, where the sequential pattern is chosen by (and subsequently remembered by) the authorized user of the card.

* US 5,259,649, wherein Shomron teaches printing a plurality of PINs on the 5 surface of a credit card and using visual cues (such as choice of font, geometric patterns adjacent the PINs, etc.) to point out the correct PIN to the authorized user.

* US 5,246,375, wherein Goede teaches the use of a matrix overlay that reveals the PIN when placed over a credit card in a predetermined orientation.

* US 4,801,787, wherein Suzuki teaches an electronic apparatus comprising a 10 memory in which the user can store easily remembered personal data (e.g., mother's maiden name) and use those data to validate his or her identity when he or she forgets the PIN.

Another area of interest to the present invention is that of telephone 15 instruments having a "speed dial" or "memory dial" capability. In these devices a user can enter a frequently called telephone number into a memory and can write some sort of name or other designation associated with that number in an enumerated list of blank fields provided on the housing of the instrument. To call the stored number, the user may consult the enumerated list to see what number is associated with the person 20 to be called, and then press a key that initiates the memory dial feature, followed by the number key on the keypad bearing the number associated with the person. It is recognised that in some such instruments (e.g., cellular phones) the number to be speed dialled is displayed on a small LCD display adjacent a keypad on a battery powered telephone instrument prior to the instrument being used to initiate the call to 25 the selected number.

One of the goals of the invention is to provide means by which a person need only remember a single identifying code and can use that identifying code to retrieve whatever such code or password is required for access to a selected secure facility or 30 transaction.

One of the benefits of the invention is that it provides escort memory apparatus that can be used by a person who requires access to a number of secure sites, equipments or transaction accounts, who has a different identifying code for

each such use, and who must enter the appropriate identifying code to gain each desired access. The invention provides the user with a small card-like escort memory device having a display; a manual data input means; a housing having a writing portion; and an electronic memory having an escort memory access code stored therein. The user may initially use the input means to enter both the escort memory access code and an identifying code associated with the each site or equipment. Subsequently, when the user desires access to the selected site or equipment he or she can enter the escort access code and then read, from the display, the identifying code needed to access the selected site or equipment. In a preferred embodiment the user can write a mnemonic descriptor (e.g., the name of a bank) on a designated blank writing portion of the housing for each stored identifying code so that the descriptor is immediately adjacent an indicium representative of a unique data record label. In one such embodiment, twenty four blank spaces are provided where each blank is uniquely associated with an integer lying in the range from one to twenty four.

15

A preferred embodiment of the invention provides a software security arrangement in which all of the identifying codes stored in a memory of the escort memory device are erased after some predetermined number of sequential inputs of trial escort memory access codes fail to match the stored escort memory access code.

20 In a particular preferred embodiment, the escort memory enters a software self-destruct mode after three erroneous codes are entered in sequence.

Moreover, a preferred embodiment of the invention provides physical means of preventing an unauthorised person from tampering with or illicitly acquiring the 25 identifying codes stored in the escort memory. These means may include providing a sealed housing that can not be opened without a high likelihood that doing so would break a circuit trace or otherwise destroy the apparatus.

Although it is believed that the foregoing recital of features and advantages 30 may be of use to one who is skilled in the art and who wishes to learn how to practice the invention, it will be recognised that the foregoing recital is not intended to list all of the features and advantages. Moreover, it may be noted that various embodiments of the invention may provide various combinations of the hereinbefore recited

features and advantages of the invention, and that less than all of the recited features and advantages may be provided by some embodiments.

To help understanding of the invention, a specific embodiment thereof will
5 now be described by way of example and with reference to the accompanying drawings, in which:

Figure 1 is a front elevational view of an escort memory apparatus of the invention

Figure 2 is a rear elevational view thereof.

10 Figure 3 is a schematic block diagram of the escort memory device.

Figure 4 depicts a flow chart that could be carried out by an escort memory of the invention and depicts flows of identity information between the escort memory and secure systems, the flows all passing through a user.

15 An escort memory apparatus 30 of the invention is preferably configured as a nearly wallet-sized card that can be carried about as easily as one could carry a credit card. Although small calculators having the same length and width as a credit card (i.e., about eighty five millimetres by fifty four millimetres) have been on the market for some time, they are considerably thicker than a credit or debit card, which is
20 commonly about one half millimetre thick. A preferred embodiment of the escort memory apparatus 30 is between two and three millimetres thick. The overall dimensions for the apparatus 30 are thus selected to be about eighty three by fifty seven millimetres by three millimetres, where the length and width are chosen to differ from normal credit card dimensions by two to three millimetres in order to
25 make the apparatus of the invention somewhat easier for a user 50 to find in his or her wallet. Additionally, the slight decrease in the width of the apparatus 30, offsets the greater thickness so that the apparatus 30 can fit into a wallet slot intended for a credit or debit card.

30 The escort memory apparatus 30 preferably comprises, as its only output, a low power display, which may be liquid crystal display 32; or may be any other such display operating with the same or lower power requirements 2E. The memory apparatus 30 has, as its only user input, a manual input device such as the preferred membrane keypad 34 depicted in the drawing. Operation of the apparatus 30 is

controlled by a control means that is preferably a microcontroller or microprocessor 36 operating under control of a program stored in a read-only memory 38. Although many different sorts of microcontrollers or microprocessors could be considered, an initially preferred apparatus of the invention 30 used a Model MSM64155 made by
5 Oki Semiconductor. In addition to the masked ROM 38, a read-write memory, such as an EEROM 40, was also associated with this microprocessor 36 and was used for storing identity codes, as will be described in greater detail hereinafter. In a subsequent embodiment of the invention an Oki Model MSM63184A microcontroller was selected. This latter device had sufficient on-board memory that the developers
10 were able to dispense with the EEROM as a separate component. In the initially preferred embodiment using the Oki Model MSM64155, eliminating the EEROM led to a device capable of storing only five codes strings if each code string was ten characters in length.

15 A preferred escort memory apparatus 30 is powered by a non-rechargeable, non-replaceable primary battery 42 that is permanently sealed into the casing or housing 44 of the apparatus so as to prohibit replacement of the battery 42. This approach to making the apparatus 30 minimises its initial cost. The tamper-resistant housing 44 also provides a measure of security, in that no one can open the housing in
20 order to attempt to read out data stored in the EEROM 40. As a further deterrent to theft by a skilled and well equipped thief, in a preferred embodiment the data stored in the EEROM 40 and in memory on the microprocessor 36 chip are encrypted.

Another feature of a preferred housing 44 is a writing area 46 disposed on the
25 back of the housing 44 and providing an enumerated, or otherwise conveniently labelled, set of defined spaces 47 wherein a user 50 can write names that he or she can use to designate a bank account, computer, etc., for which he or she wants to remember a password or other identifying code. The writing area 46 may be formed as a roughened portion of a plastic housing, may be an adhesive-backed paper form
30 adhered to the housing, or may be formed by any other known approach allowing someone to write short text strings thereon by the use of conventional writing implements.

Turning now to Fig. 4, one finds a depiction of the use of an escort memory 30 by a user 50 to store and to retrieve a plurality of user-identifying codes. Each of these codes is respectively associated with a separate secure system 52. The exchange of data between the user 50 and the various apparatuses 30, 52 is indicated in Fig. 4 with the bold arrows 53. As is well known in the art, each of the systems 52 issues a password, PIN, or other identity code (depicted as PIN 1 to PIN N in Fig. 4) to the user 50 and then requires the user to input that code in order to access the system 52. The user 50 can store the identity codes PIN 1 . . . PIN N in the escort memory apparatus 30 by entering a trial escort access code as shown in Step 54. The program running in the escort memory apparatus 30 compares the trial code with an escort access code 56 stored in the EEROM 40, as indicated in Step 56. If the user enters the correct escort access code, he or she can then choose (Step 58) to either store a new identity code (Step 60) or to read a previously stored code (Step 62) from the memory 40.

15

In order to prevent a thief from guessing the stored access code in a stolen escort memory device 30 a limit is placed on the number of allowable comparisons made in Step 56 between a trial escort access code and the stored escort access code. If a predetermined maximum allowable number of attempts to match the codes is reached, the program enters a software self-destruct or failure mode (Step 64). In a preferred embodiment, the maximum number of attempts to match the stored escort access code is set at three, and the failure mode completely and permanently disables the apparatus 30 by erasing or over-writing all of the stored identity codes and the stored escort access code.

25

In a specific preferred embodiment, the escort apparatus 30 is supplied to an end user with a factory set escort access code (e.g., "877"). The user 50 is directed to begin his or her use of the apparatus by over-writing the factory generated and generally publicly known escort access code with an escort access code of his or her own choosing. This may be done by turning on the apparatus 30, which is programmed to initially read the stored escort access code, and, if that access code is the initial factory set code, to allow the user complete access to data stored in the device. Alternately, of course, the device could be programmed to display the same start-up message used in normal operation - e.g., "enter code", and the user could first

enter the factory code (which can be printed on a temporarily adhered tag), and then begin an escort access code change routine (e.g., by simultaneously pressing two keys, or by entering a code entry sequence, such as the "PGM" key followed by "00").

5 After gaining access to the escort apparatus 30 by entering his or her escort access code, the user can enter one or more identity codes. For example, he or she could select a data field by keying in a unique record label and pressing the "PGM" key, which would result in the display of the unique record label designation 45 on the display. In a preferred embodiment the unique record label designation 45 is a two
10 digit prompt, where the two digits (commonly the integers lying in the range of one to twenty, where the integers between one and nine are displayed with a leading zero) represent a memory location available for storage of a uniquely labelled data record. He or she could then use the keypad 34 to enter the desired identity code or PIN, which would be displayed as it was entered. After checking the display to ensure that
15 the correct code was entered, the user would press the ENT key to write the code into the memory location operatively associated with the two digit prompting message. Before or after this step the user would preferably write a user-generated mnemonic designation in a corresponding space 47 in a writing area 46 on the back of the housing 44. It will be recognised that many variations on this data entry process are
20 possible, and that the one cited above is merely one of several convenient choices. It may also be noted that the apparatus 30 can be configured to allow the entry of only one PIN for each entry of the access code, or may allow entry of any number of PINs once it has accepted a valid access code.

25 For the more common operation of consulting the escort apparatus 30 in order to retrieve an identity code for use with a secure system (e.g., an automatic teller machine from which the user wants to withdraw cash from a bank at which he or she has an account), the user would switch the escort apparatus into its active mode, enter his or her escort access code, and then select the identity code display function (e.g.,
30 by pressing the ENT key on the keypad). In a preferred embodiment the display then shows the PIN stored in the first memory location in the format "01.nnnnnnnnnn", where the dot or other separator separating the memory location designation "01" from the access code "nnnnnnnnnn" may be printed on a overlay aligned with the LCD display 32 in order to avoid having to give up a portion of the LCD for the

display of repetitive material. At this point in the preferred sequence, the user refers to the list of mnemonic designations (e.g., the name of the bank) and inputs the two digit number associated with that designation in the enumerated list of names appearing on the back of the apparatus, and again presses "ENT" to display the 5 requested identity code. It will be noted that many other arrangements, e.g., displaying a prompting message at start-up rather than showing the contents of the first memory location, or allowing the user to scroll sequentially through all the stored identity codes, could also be used for identity code retrieval and display.

10 The preferred apparatus is expected to have only a limited memory capacity - e.g., it may store only one escort access code and twenty separate identity codes, where each code is up to twelve alphanumeric characters in length. Hence, an appropriate arrangement will be made for deleting or for over-writing old identity codes with new ones whenever a user changes banks, or is issued a new password for 15 a computer used at work, etc. A preferred process of doing this comprises the steps of: a) gaining access to the apparatus 30 by entering the appropriate escort access code, b) entering the data field number associated with the account and hitting the "PGM" key; c) entering the new identity code datum followed by the "ENT" key. A similar approach may be used to change the escort access code. In this case, instead 20 of entering a number associated with a data field, the user enters a selected number, such as "00", that is not within the range of numbers used to identify data fields (e.g., is not one of the integers between one and twenty).

25 A preferred operating program also uses an internal timer to automatically turn off the display and place the apparatus in a low power mode of the sort commonly called "sleep mode" after a short period (e.g., fifteen seconds) of inactivity. As is known in the art, the period of inactivity may be measured from the time that a manual input places the apparatus in its active mode, or, more commonly, may be measured from the time that the most recent user input is supplied at the keyboard. 30 The use of this dual mode operation is important to the present invention for several reasons. Because the device is expected to be a low cost device to be used only until the battery is depleted and then thrown away and replaced, sleep mode operation is important in prolonging the life of the apparatus. Additionally, the provision of a timed operating cycle allows for simpler operation in that the user does not have to

learn any additional steps to turn the apparatus off. All he or she needs do is place the apparatus in a pocket or purse and it will automatically enter sleep mode and refuse to display stored identity codes until the stored escort access code has again been entered. Moreover, a preferred embodiment of the apparatus employs a small

5 "telephone-type" keypad in the interest of reducing both size and cost and preferably uses one of the keys in the keypad (e.g., the "5" key in the middle of the pad is pressed twice within three seconds) to cause the microprocessor to enter its active mode in which inputs are accepted and outputs displayed. This sort of arrangement avoids adding a dedicated ON/OFF switch to the unit.

10

As is known in the art, a telephone-type a keypad can be used for alphanumeric and special character data entry by using repetitive keystrokes to enter a selected one of the letters displayed above a numbered key. For example, a letter "e", which is the second letter in the "DEF" triad associated with the "3" key can be
15 entered by hitting "3" key three times in succession.

Like many other relatively low cost products, the apparatus of the invention may also find use as an advertising specialty item bought in large numbers by a single company and then given away to that company's customers or prospective customers.

20 In a preferred advertising specialty embodiment of the invention, a corporate logo, trademark emblem or other identifying indicium 66 is imprinted on the housing 44 of each storage apparatus 30 of a custom ordered lot thereof. Moreover, a brief advertising message comprising a string of alphabetic or alphanumeric characters may be stored in a predetermined portion of the memory 40 and displayed to the user of
25 the apparatus 30 each time it is turned on. For example, the apparatus described above that could contain up to twenty PINs can be reprogrammed to serve as an advertising specialty product by dedicating the memory space otherwise used by four of the twenty identity codes to an advertising message or other message unrelated to identity codes. This message, which could be over thirty characters in length, is then
30 scrolled across the twelve character display 32 whenever the apparatus 30 is turned on and before the user enters his or her access code. It will be appreciated by those skilled in the computer arts that the same hardware can be used for either application. Customising a batch of escort memory devices 30 can be done before packaging the apparatus by selecting the program to be stored in the microprocessor's ROM 38,

storing an advertising message unrelated to any identity code that is to be used in the data memory 40 and by arranging for printing, engraving, or otherwise displaying custom indicia on the outside of the housing 44.

5 Alternately, the apparatus 30 can be customised after sealing by using a connector comprising a thin contact insertable into a connector in the housing to make electrical contact to appropriate circuit points. This arrangement permits a retailer to use the special writing apparatus to economically add advertising, promotional, or other messages to ones of a relatively small lot of apparatuses 30. In a preferred
10 arrangement, the writing apparatus is configured to have an interface to a desktop computer capable of running the writing software and of displaying the message to be written before it is entered into the apparatus 30.

Although the present invention has been described with respect to several
15 preferred embodiments, many modifications and alterations can be made without departing from the invention. Accordingly, it is intended that all such modifications and alterations be considered as within the spirit and scope of the invention as defined in the attached claims.

20 The invention provides apparatus and method for conducting secure financial transactions and for acquiring access to secured facilities and equipment.

CLAIMS

1. Apparatus for storing an escort access code and up to a predetermined number of identifying codes, each of the identifying codes respectively associated with a user-generated designation, the apparatus characterised in that:

- 5 • a computer memory (40) is controlled by a microprocessor (36) to store, at respective locations therein, the escort access code and each of the identifying codes;
- 10 • a display (32) is controlled by the microprocessor (36) to display one of the identifying codes during a predetermined interval after the user supplies the escort access code to the microprocessor by means of a keypad (34); and
- 15 • a writing area (46) is disposed on a portion of a housing (44) that encloses the microprocessor (36), a battery (42) and the computer memory (40), the writing area adapted to have the user-generated designation written thereon.

2. The apparatus of Claim 1 wherein the microprocessor has both a sleep mode
15 and an active mode.

3. The apparatus of Claim 1 wherein the memory is further adapted to store a message unrelated to any of the codes, and wherein the microprocessor is adapted to retrieve the unrelated message and control the display to display the unrelated message whenever the microprocessor switches from a sleep mode to an active mode.

20 4. The apparatus of Claim 1 wherein the housing is tamper-resistant and is adapted to prohibit replacement of the battery, and wherein the battery is a primary battery.

5. The apparatus of Claim 1 wherein the computer memory comprises an EEPROM.

25 6. A method for storing and retrieving a user-identifying code that is to be supplied to a secure apparatus in order to obtain access thereto, the method comprising the steps of:

- 30 a) storing, in an escort memory apparatus that requires entry of a trial access code matching a stored escort access code before displaying the identifying code, the user-identifying code as a record uniquely associated with a respective record label;
- b) supplying, by means of a manual input to a keypad, the trial access code to the escort memory apparatus;

c) reading a first message displayed by the escort memory apparatus and, if the first message indicates that the trial access code matches the escort access code, entering, by means of the keypad, the label uniquely associated with the user-identifying code; and

5 d) reading the user-identifying code displayed by the escort memory apparatus responsive to the input of the unique record label.

7. The method of Claim 6 further comprising a step subsequent to step a) and prior to step b) of:

10 • writing a user-generated designation associated with the secure apparatus on an external portion of the escort memory apparatus, the external portion adjacent indicia representative of the unique record label.

8. The method of Claim 6 wherein the escort memory apparatus stores a second message, unrelated to any of the codes, and displays the second message prior to step b).

15 9. The method of Claim 6 wherein, if the trial access code supplied in step b) does not match the escort memory access code, the first message indicates to the user that a first repetition of step b) is required and, if the trial access code entered in the first repetition of step b) does not match the escort access code, a second message is displayed indicating that only one more repetition of step b) is allowed before the
20 escort memory apparatus erases all stored codes.